Problématique des identifiants/uid

Sylvain.Brachotte@uhp-nancy.fr

tutoJRES 11

Annuaires : mise en oeuvre de SupAnn 2008

Les Identifiants

2. Définition de la notion d'identifiant
   - Qu'est ce qu'un identifiant ?
   - Que choisir comme identifiant ?
   - Que peut on prendre comme identifiant ?
3. Les identifiants SupAnn 2008
   - Uid, SupannAliasLogin, eduPersonPrincipalName
4. Analogie avec les identifiants de documents pérenne BNF
5. Mise en oeuvre inter établissements (Nancy Université)
6. Les identifiants opaques
7. Les implications pour l'avenir ?

Définition de la notion d'identifiant

- Sur wikipédia
  - En informatique, on appelle identifiants (également appelé parfois en anglais login) les informations permettant à une personne de s'identifier auprès d'un système.
  - Il s'agit le plus souvent des informations suivantes :
    - » un nom d'utilisateur
    - » un mot de passe
  - Les termes désignant l'opération consistant à donner ces informations au système peuvent varier selon le contexte. Ainsi on peut retrouver les termes suivants :
    - » connexion à une base de données : se connecter/se déconnecter
    - » identification, authentification : s'identifier, « se loguer » ou se déconnecter , « se déloguer » (issu de l'anglais to log in ou to log on).
  - http://middleware.internet2.edu/internet2-mi-best-practices-00.html

Les identifiants SupAnn V1 (1)

Trois attributs permettent de gérer les identifiants
Il s'agit de uid, eduPersonPrincipalName et supannAliasLogin.

- **uid** a plusieurs rôles :
  - 1. RDN de l'entrée de l'utilisateur
  - 2. il peut aussi s'agir du « login » dans des applications traditionnelles (non Web) ou des systèmes d'exploitation (login UNIX).

- **eduPersonPrincipalName** contient l'identifiant institutionnel de la personne. Il est de la forme **idperso@domaine**.
  - id-perso respecte des règles définies par l'établissement.
  - Cet identifiant est stable dans le temps mais peut être modifié sur demande de l'utilisateur dans des cas particuliers comme un changement de nom d'usage suite à un mariage.

Les identifiants SupAnn V1 (2)

- **supannAliasLogin** contient un identifiant choisi par l'utilisateur et connu de lui seul (il n'est jamais affiché par des applications).
  - Il lui permet de saisir, lorsqu'il se connecte à son ENT un identifiant plus court que l'institutionnel ou auquel il est habitué. Toutefois, supannAliasLogin doit être unique dans l'établissement et cette unicité est gérée selon la règle « premier demandeur, premier servi ».
  - Remarque : eduPersonPrincipalName et supannAliasLogin ont été prévus principalement pour les espaces numériques de travail (ENT) mais peuvent être utilisés dans un cadre plus large.

Les identifiants SupAnn 2008

- Les recommandations SupAnn 2008 définissent plusieurs attributs candidats devant être utilisés comme identifiant de personne.
  - **uid** (Unique IDentifier) : identifiant de l'utilisateur dans le système d'information.
  - **eduPersonPrincipalName :** identifiant de personne, globalement unique. Pour ce faire, il est constitue de deux parties, séparées par le caractère '@'. La partie gauche doit être unique pour un établissement donné ; la partie droite qualifie l'établissement.
    En revanche, la partie droite **DOIT** correspondre au domaine DNS de l'établissement.

    Cet attribut n'a pas vocation à être directement manipulé par les utilisateurs (**un utilisateur n'est pas censé connaitre la valeur de son eduPersonPrincipalName**).

    En revanche cet attribut pourra être utilisé par une application pour faire référence (par exemple pour gérer des règles de contrôle d'accès) à des utilisateurs issus d'un autre établissement.

Les identifiants SupAnn 2008 (2)

- **supannAliasLogin** : chaine de caractères, associée à un mot de passe, utilisée par l'utilisateur pour s'authentifier.

  Par défaut il correspond à l'attribut uid.

– **uid**

- Sémantique : **identifiant unique**
- Origine : **RFC2798**
- Valuation : **multivalué mais ne devrait contenir qu'une valeur**
- Obligatoire : **Demande**
- Contenu : **DOIT être utilisé comme RDN pour les entrées de personnes, contenu indifférent.**
  - Comme l'attribut uid peut être utilisé comme identifiant dans des applications, il est important que la valeur de cet attribut ne soit pas réassignée à une autre personne d'une année à/sur l'autre.
  - **L'utilisation d'un uid d'utilisateur incrémental et opaque peut aider à atteindre cet objectif.**

Les identifiants SupAnn 2008 (3)

- **eduPersonPrincipalName**
  - Sémantique : **Identifiant institutionnel unique**
  - Origine : **Internet2 (eduPerson)**
  - Valuation : **Monovalué**
  - Obligatoire : **Non**
  - Contenu : **nom qualifie de la forme <identifiant local>@<domaine>**
    - Comme l'attribut eduPersonPrincipalName peut être utilisé comme identifiant dans des applications, il est important que la valeur de cet attribut ne soit pas réassignée à une autre personne d'une année à/sur l'autre.
    - **L'utilisation d'un identifiant d'utilisateur incrémental et opaque peut aider à atteindre cet objectif.**
    - Cet attribut ne doit pas être confondu avec l'attribut **mail dont la syntaxe proche.**

Les identifiants opaques

- Présentation de « *Des identifiants pérennes pour les ressources numériques* » de Emmanuelle Bermès Bibliothèque nationale de France (*jres 2007*)

    - Identifiants signifiants
        - » nla.ms-ms51-1 pour la série 1 des Papiers de Sir EdmundBarton
    - Identifiants opaques
        - » urn:hdl:loc.pnp/gsc.5a14460

  – Critères attendus pour les identifiants
    – Unicité : l'identifiant désigne une ressource et pas une autre
    – Pérennité : l'identifiant ne doit pas dépendre de l'emplacement physique de la ressource
    – Granularité : l'identifiant est applicable à plusieurs niveaux
    – Adaptabilité/Extensibilité : l'identifiant doit s'adapter à des modèles préexistants

Les apports des attributs opaques pour les identifiants de personne dans nos SI

- Gagne sur l'espace de nommage (plus grand)
- Gagne sur la non réutilisation des attributs
- Pas de soucis de conflit, doublon, de réallocation, d'erreurs d'attribution ou d'aiguillage, d'homonymie …
- Génération automatique des identifiants
- Procédure interne externalisable, distribuable, le Réferentiel pourrait les attribuer lors de la création d'une ressource.

Un exemple concret

- Une nouvelle utilisatrice : **Arlette Besanceno** de l'université : mon-univ.fr
- Avec SupAnn V1 :
  - Uid : abesan12
  - supannAliasLogin : abesan12
  - eduPersonPrincipalName : abesan12@mon-univ.fr
  - Mail : arlette.besanceno@mon-univ.fr
  - DisplayName : Arlette Besanceno
- Avec SupannV2008 :
  - Uid : identifiant_opaque (ETU/PERS_1234567)
  - supannAliasLogin : arlette (si pas utilisé dans l'établissement)
  - eduPersonPrincipalName : identifiant_opaque@mon-univ.fr
  - Mail : arlette.besanceno@mon-univ.fr
  - DisplayName : Arlette Besanceno

Etude de cas concret

- Contexte :
  - Nouvel établissement : EPCS Nancy-Université
  - Union de 3 établissements nancéien
    - » Université Henri Poincaré
    - » Université Nancy 2
    - » Institut National Polytechnique de Lorraine

  - Accès aux ressources communes par les étudiants des trois établissements, sans avoir un quatrième établissement à gérer.
  - Mise en œuvre sans bouleverser les systèmes d'informations existants.
  - Première réflexion sur la population « étudiante » avant d'avoir une unicité des identifiants pour tout le monde sur la plaque nancéienne.

Etude de cas concret (2)

- Existant dans chaque établissement :
  - Un ou des annuaire(s) supann
  - Un logiciel de gestion de la population étudiante : Apogée
  - Des procédures internes

  - **UHP :**
    - Identifiant sur 8 caractères maxi (5 premiers du nom + un nombre)
    - Un process spécifique à partir de la base métier Apogée (identifiant, mail, Active Directory, Home, …, Charte Informatique …)
  - **Nancy2 :**
    - Identifiant sur 8 caractères (5 premiers du nom + un nombre sur 3 chiffres)
    - Un process spécifique à partir de la base métier Apogée (trigger) (identifiant, mail, …)
  - **INPL :**
    - Identifiant sur 8 caractères maxi (5 premiers du nom + un nombre aléatoire)
    - Un process spécifique à partir de la base métier Apogée (identifiant, mail, …)

- Le **système actuel** (mis en œuvre) :
  - Chaque établissement continue de gérer sa population d'étudiants,
  - Politique commune de nommage des identifiants des étudiants,
  - Mise en place de la brique shibboleth pour les applications type e-learning,

  - Format commun : sur **9 caractères**
    - **5** premiers caractères du NOM + 1 nombre de **3** chiffres (000 – 999) + **1** nombre identifiant de l'établissement d'origine
  - Pas de grosses modifications dans les procédures
    - UHP : (identifiant 1)
      - » Trigger Apogée : affecte le login : dupon0051
    - Nancy2 : (identifiant 2)
      - » Trigger Apogée : affecte le login : dupon0052
    - INPL : (identifiant 3)
      - » Procédure interne : affecte le login : dupon0053
  - Début de réflexion sur les autres catégories de personnel :
    - L'uid de la personne est celui de l'établissement d'origine.

Les identifiants opaques, questions ouvertes

- Pourquoi pas un seul et unique identifiant au niveau national
  - uid= **{code UAI}+base_metier+identifiant,ou=people,dc=mon-univ,dc=fr**
  - eduPersonPrincipalName={code UAI}+base_metier+identifiant@mon-univ.fr
- Pourquoi pas un uid totalement abstrait avec une clé de vérification
  - Valable dans tous les établissements, unicité, transportabilité, pas de doublon …
- Pour la population qui quitte l'établissement
  - On garde l'uid dans le ou les annuaire(s)
  - On renseigne le mail avec celui de mail de destination, ou le mail personnel
    - Pour tout ce qui est accès physique : type (ent, listes de diffusion, ressources en ligne) la personne s'identifie avec son mail (sésame type openid)
    - La personne reste en contact puisque redirection de la messagerie vers la nouvelle adresse mail
    - La personne reste dans l'annuaire, donc pour les enquêtes suivis de carrières « pas de soucis »
    - Le Système d'Information ou le référentiel pourra réutiliser les attributs SupannAliasLogin et Mail (après un certain temps)
- A quand un mail permanent @education.gouv.fr ?

Les identifiants opaques, questions ouvertes (2)

- Couplage Annuaire – système de messagerie
  - On déplace le problème de l'uid = login
  - Réutilisation impossible des logins déjà attribués, sauf si opaques aussi.
- Identifiant national
  - Uid : {UAI} + base_metier + identifiant_individu
  - eduPersonPrincipalName : {UAI} + base_metier + identifiant_individu@domaine
- Pourquoi pas des identifiants de type « ine » pour les étudiants et « numen » pour les autres types de personnels ? A la condition que la gestion de l'unicité soit gérée de façon à éviter les changements d'uid, ou les renommages….
- Quid d'une migration vers des identifiants opaques …